Effective IT Strategies and Tools for remote work in preparation for COVID-19 Disruption

Below is an IT checklist for being prepared and ready to work remotely:

- Reliable home or remote network connectivity
  If you do not have internet access at home, consider purchasing a prepaid hotspot such as the Verizon Ellipsis Jetpack, the AT&T Velocity Hotspot, or others.
  IS&T(servicedesk@mit.edu) has a handful of loaner iPads with cellular service for faculty and staff

- OVC DS-issued laptop or a personal computer with the latest Operating System
  Install MIT Certificates on Personal Computer (https://ca.mit.edu/ca)

- Familiarity with where your work-related data is stored
  File Shares
  MIT Dropbox or OneDrive
  Google Drive

- Installed communication/collaboration tools to connect with peers and colleagues (preinstalled on all OVC DS-issued machines)
  Slack
  WebEx (https://ist.mit.edu/conferencing)
  Zoom

- Desk Phone Call Forwarding
  Click here for instructions or here for a video demo
  Or contact MIT HelpDesk at: servicedesk@mit.edu

- Register Multiple Devices for Duo (Two Factor Authentication)
  https://duo.mit.edu

- Connect to MITNet Via Cisco AnyConnect VPN

  MIT VPN is the core foundation for secure Internet access.
  Additionally, you need to use the MIT VPN from off-campus to connect to:

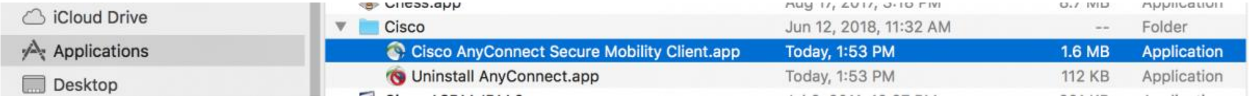
  MITSIS
  PowerFAIDS
  BrioQuery
  SAP
  Data Warehouse (FileMaker)

Fileservers

All OVC/DSL Laptops have Cisco AnyConnect VPN Installed.
To use Cisco Any Connect VPN services off-campus, you must have internet access.

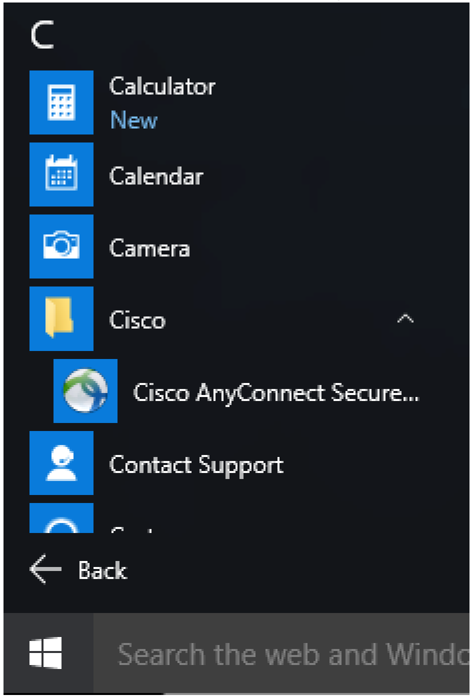
To Connect (comes from IS&T):

Macs: Launch the Cisco AnyConnect Secure Mobility Client from your Applications folder (/Applications/Cisco/):

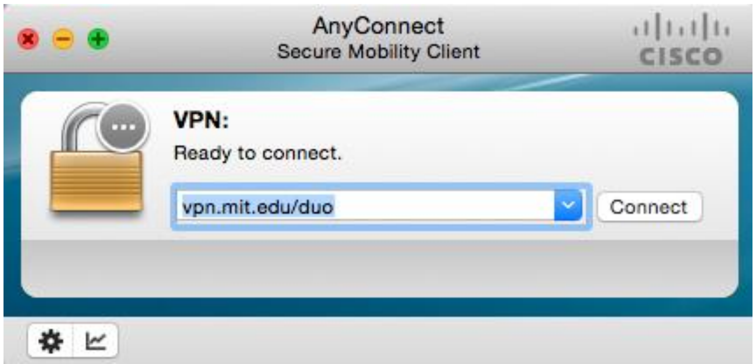


▼ Cisco	Jun 12, 2018, 11:32 AM	--	Folder
Cisco AnyConnect Secure Mobility Client.app	Today, 1:53 PM	1.6 MB	Application
Uninstall AnyConnect.app	Today, 1:53 PM	112 KB	Application

PCs: Launch the Cisco AnyConnect Secure Mobility Client from the Start Menu:



To authenticate with DUO, enter vpn.mit.edu/duo and click the Connect.

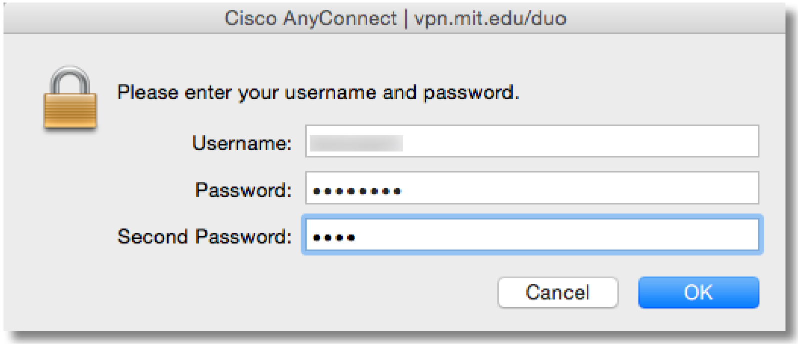


AnyConnect
Secure Mobility Client

VPN:
Ready to connect.

vpn.mit.edu/duo

“Username” And “Password” are Your MIT Login Credentials (Kerberos and Kerberos password).



Cisco AnyConnect | vpn.mit.edu/duo

Please enter your username and password.

Username: [redacted]
Password: ••••••••
Second Password: ••••

For the “Second password”, type the following options then click OK*:
push - Duo will send a push notification to your registered cell phone with the Duo Security mobile app installed
push2 - Duo will send a push notification to your second registered device with the Duo Security mobile app installed
sms - Duo will send an SMS to your registered cell phone
Phone -Duo will call your registered phone
Phone2 -Duo will call your second registered phone
YubiKey - If you are using a YubiKey for authentication, make sure the Second Password field is highlighted and use your key. For instructions on using the YubiKey, please see How do I authenticate with a YubiKey?
The one-time code generated by your hardware token or the Duo Security mobile app (the code changes every 60 seconds)
Cisco AnyConnect should now present you with an MIT VPN Banner and accept the VPN connection to complete.

*OVC Desktop Support strongly recommends that you register an alternative device for Duo authentication (if you only registered your office phone or if something happens to your registered device). To register a backup device, go to https://duo.mit.edu or request a YubiKey token here.